



Citrix Home User Guide

Defense Logistics Agency

User Guide and Operational Procedures for Citrix

Version 1.11

Date: August 27, 2012

FOR OFFICIAL USE ONLY

Table of Contents

1. About This Guide..... 3

 1.1. Who Should Use It 3

2. Citrix – Introduction.....4

 2.1. Overview..... 4

 2.2. Hardware and Software Required 4

 2.3. Help Desk Support.....5

3. Pre-connection and Configuration Activities..... 6

4. Establishing a Citrix Connection..... 14

Appendix A – How to Establish Outlook Profile Settings22

Appendix B – Printing With Citrix..... 23

Appendix C – Tips and Common Error Solutions 24

Appendix D - Instructions for Configuring and Using Citrix with Mac OS.....30

Appendix E – Approved Smart Card Readers.....45

Version History

Version	Description	Author	Date
1.7	Mac OS updates included	Damon Gatewood	June 5, 2012
1.8	Table of Contents, footers and screenshots updated to remote.dla.mil site	Kellie Clark	June 8, 2012
1.9	Additional updates	James Hasenbein	June 12, 2012
1.10	Additional updates	James Hasenbein	July 30, 2012
1.11	Updated Login Page	Gary Herchek	August 27, 2012

1. About This Guide

1.1. Who Should Use It

This user guide is intended to provide Defense Logistics Agency (DLA) personnel with instructions and operational procedures to connect to the DLA network via Citrix, using non-Government-Furnished Equipment (non-GFE). Non-GFE includes both Contractor-Furnished Equipment (CFE) and personal equipment (i.e., home computer).

Risks

There are potential risks associated with installing prerequisite software components (i.e., ActivClient, Citrix Online Plug-in, DOD Root Certificates) and using the remote access system. It is not possible to test these components with all software and/or applications that are commercially available and that may be on your home computer. Therefore, it is possible that the prerequisite software components could conflict with other applications or software residing on your home computer. Use of this capability on your personal non-Government-furnished computer is at your own risk.

Disclaimer of Liability

With respect to installing prerequisite software components or using the remote access solution, neither the DOD, DLA, nor any employees within, provide any warranty, expressed or implied, or assume any legal or financial liability or responsibility for your non-Government computer system and/or damages or repairs that may result from system incompatibilities with the remote access solution. By installing prerequisite software and using this product, you signify your agreement to the preceding terms and conditions. If you do not agree to these terms and conditions, do not install or use this product.

2. Citrix – Introduction

2.1. Overview

Citrix provides a secure means of teleworking using a remote user's personal or contractor-furnished computer. Citrix contains security configurations to prevent access to the user's local storage devices (i.e., hard drives and flash drives). Users connect to Citrix via their Web browser, enabling easy and secure access to available DLA applications as only keystrokes, mouse clicks, and display images are transmitted over an encrypted connection between the client computer and the Citrix environment.

2.2. Hardware and Software Required

Personal or contractor-furnished devices running on Windows XP, Windows Vista, Windows 7 or the latest versions of Mac OS can be used via the processes described in this document. The table below is a breakdown of all browser/operating system combinations that are supported by Citrix. It is highly recommended to use one of these combinations, as deviation could result in performance issues or inability to connect.

Browser	Operating system
Internet Explorer 8.x (32-bit mode)	Windows 7 64-bit Editions
	Windows 7 32-bit Editions
	Windows XP Professional with Service Pack 3
	Windows XP Professional x64 Edition with Service Pack 2
	Windows Vista 32-bit Editions with Service Pack 2
	Windows Vista 64-bit Editions with Service Pack 2
Internet Explorer 7.x (32-bit mode)	Windows Vista 64-bit Editions with Service Pack 2
	Windows Vista 64-bit Editions with Service Pack 2
	Windows Vista 32-bit Editions with Service Pack 2
	Windows Vista 64-bit Editions with Service Pack 2
Safari 5.x	Mac OS X Snow Leopard 10.6

Browser	Operating system
Safari 4.x	Mac OS X Leopard 10.5
Mozilla Firefox 4.x (32-bit mode)	Windows 7 64-bit Editions Windows 7 32-bit Editions Windows XP Professional with Service Pack 3 Windows XP Professional x64 Edition with Service Pack 2 Windows Vista 32-bit Editions with Service Pack 2 Windows Vista 64-bit Editions with Service Pack 2
Mozilla Firefox 3.x	Mac OS X Snow Leopard 10.6 Mac OS X Leopard 10.5 Windows XP Professional x32 Edition with Service Pack 3 Windows Vista 32-bit Editions with Service Pack 2 Windows 7 32-bit Editions Red Hat Enterprise Linux 5.4 Desktop

Additionally, there are three software components that are required in order to use Citrix - these are documented in Section 3 of this document.

Lastly, it is highly recommended that you use a high speed Internet connection, as opposed to dial-up or satellite.

2.3. Help Desk Support

All liability for issues and troubleshooting non-GFE lies with the end user. The DLA Help Desk will not provide support for issues with hardware/software not provided by DLA, including but not limited to non-GFE hardware, non-DLA networks (e.g., home routers, public hot spots), non- GFE printer configuration, and non-DLA software compatibility issues with Citrix.

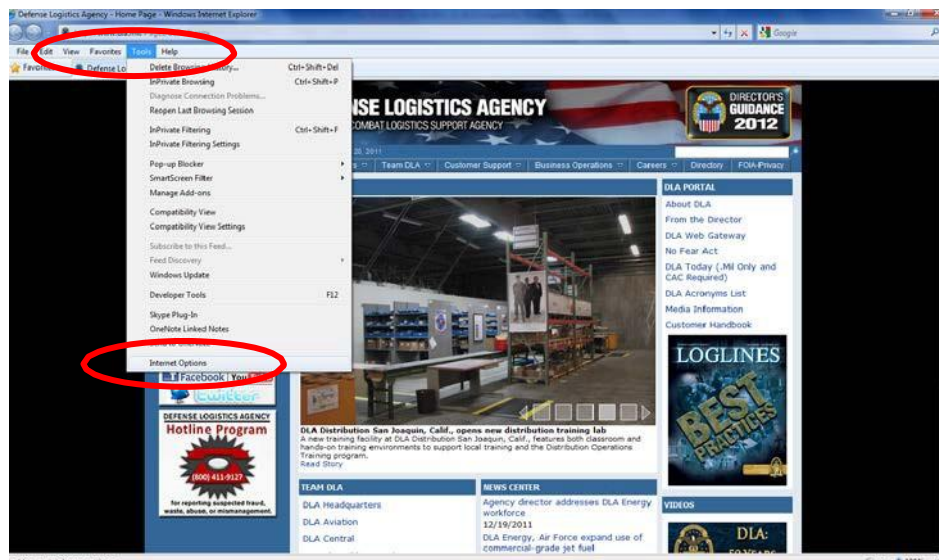
DLA Help Desk resources will support troubleshooting issues that are not related to the non-GFE hardware/software, including but not limited to accounts, DLA applications, and server-side issues.

3. Pre-connection and Configuration Activities

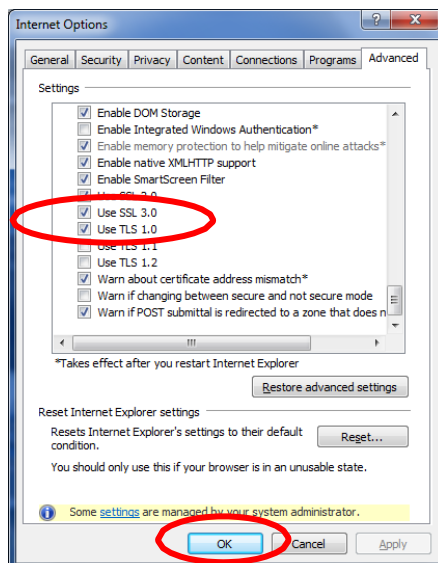
Before connecting to Citrix for the first time, certificates and client software, available on the DLA Enterprise Remote Access log-in page, need to be installed, followed by a machine reboot. This process is described in the following steps:

1. Connect your Common Access Card (CAC) Reader to an available USB Port on your Personal Computer System (Desktop/Laptop)
2. Turn on Personal Computer System (Desktop/Laptop).
3. Launch Internet Explorer V.7 or higher
4. Validate that required security protocols are enabled:

From Internet Explorer, select **Tools** and **Internet Options**



When the Internet Options window appears select the **Advanced** tab and ensure **Use SSL 3.0** and **Use TLS 1.0** are checked in the Security section.



Once these protocols are checked, click **OK**, close your Internet browser, and open a new Internet browser window.

5. Insert DLA CAC into CAC Reader
6. In your Internet browser, navigate to the DLA Enterprise Remote Access login page (URL below) to access pre- requisite files for download. Note that regardless of which DLA field site you are assigned to, everyone should obtain these files from this site.

Type the following URL and click **Enter**

<https://remote.dla.mil>

The first time navigating to this page, the user may see a warning message similar to the Web site below. If this appears, select **Continue to this Web site (not recommended)**



7. Select the **I Agree with the Statements Above** button



The screenshot shows the Defense Logistics Agency (DLA) login screen. At the top, there is a header with the DLA logo and the text "DEFENSE LOGISTICS AGENCY" and "The Warfighters Logistics Combat Support Agency". Below the header, there is a blue banner with the text "Hardware Textiles Medical Clothing". The main content area is white and contains the following text:

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

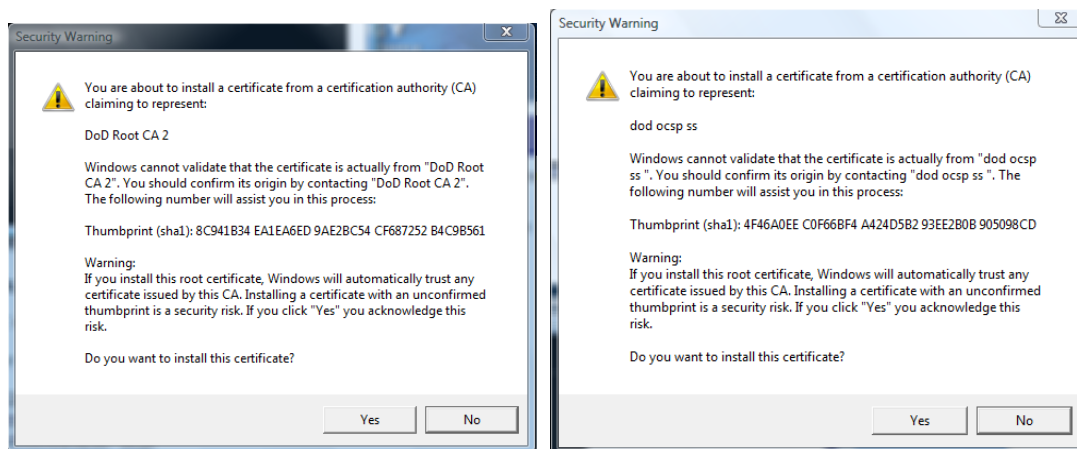
- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE, or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communication and work product are private and confidential. See User Agreement for details.

At the bottom of the screen, there are two buttons: "I Agree With The Statements Above" and "I Disagree". The "I Agree With The Statements Above" button is circled in red.

8. On the screen below you will see three links for components that need to be installed prior to establishing a connection to Citrix from each machine for the first time:



Select DOD Root Certificates -> Windows and select **Save** when prompted. Save this file to your computer, and after download is complete, locate file, right click on file, and select **Run as Administrator**. This exe file will install all required DOD Certificates to the appropriate location on your machine. These certificates are required to be installed on a machine when using a CAC. You may see two prompts issuing a security warning. These warnings are standard, and if the you accept them, should click **Yes** on both. Note that clicking **No** will prevent the machine from using Citrix.



9. On the same page, select Citrix Online Plug-in

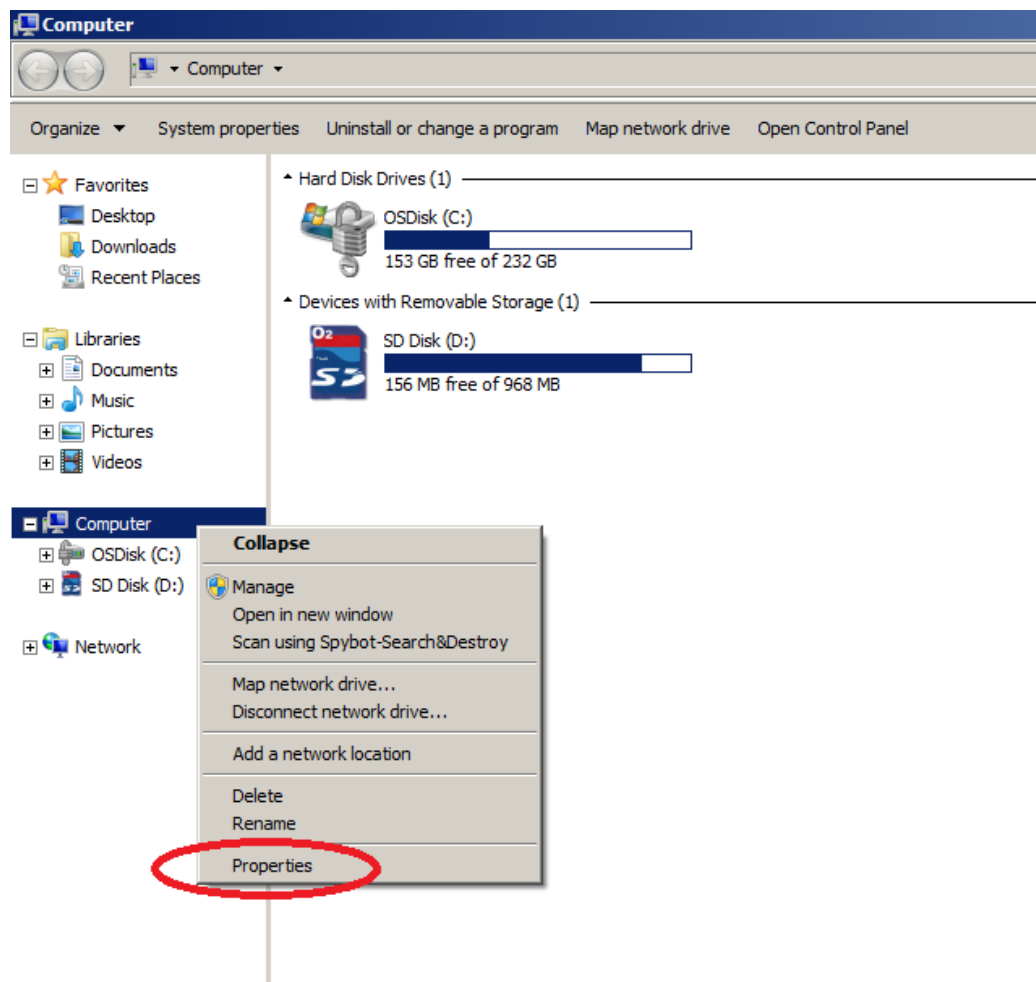


The Citrix Online Plug-in is required to establish a secure connection with Citrix. This client supports Windows XP, Vista, and Windows 7 operating systems. When prompted, run the file and accept all defaults.

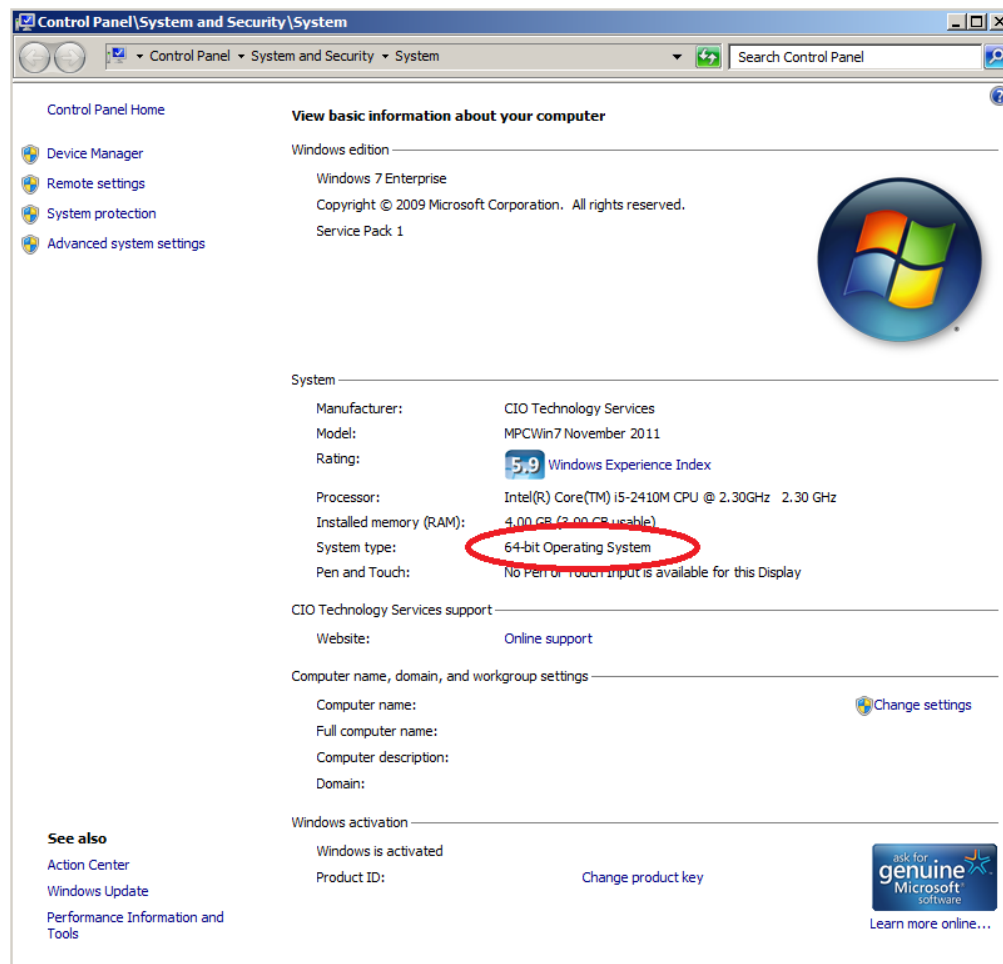
10. On the same page, you will need to install ActivClient as well as the latest hotfix. Note there are two choices of ActivClient to install, which is based on the configuration of your operating system:

- 32-Bit
- 64-Bit

You can verify the version of your operating system by right-clicking the My Computer icon on your Desktop, and selecting Properties.



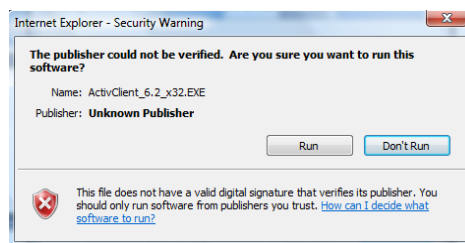
On the Screen that appears, it should state 32-bit or 64-bit Operating System.



Once your operating system type has been confirmed, select the link to download the appropriate ActivClient:



When prompted, run the install file and accept all defaults:



11. Reboot the computer after all prerequisite components have been installed.
12. Repeat Step 10 and 11 however select the hotfix instead of the Base Install.

4. Establishing a Citrix Connection

Note: Specific screenshots and images throughout this document may differ from site to site

The following steps detail the process for connecting to Citrix and launching applications once the prerequisite steps in Section 3 have been addressed.

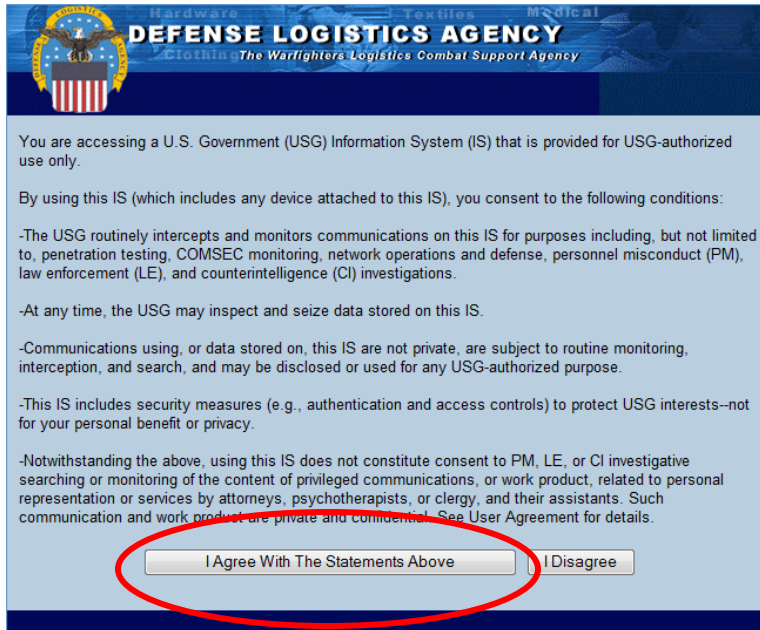
1. Connect your Common Access Card (CAC) Reader to an available USB Port on your Personal Computer System (Desktop/Laptop)
2. Turn on Personal Computer System (Desktop/Laptop).
3. Launch Internet Explorer V.7 or higher
4. As an alternative to <https://remote.dla.mil>, the following URL addresses can be accessed as listed below:

If you work at this DLA Site	Use this URL
Headquarters	https://fortbelvoir.citrix.hq.dla.mil
Aviation	https://rmt.aviation.dla.mil
Land and Maritime, Transaction Services, Logistics Information Services	https://remotec.dla.mil
Troop Support, Information Operations Ogden, Document Services	https://pubctx.troopsupport.dla.mil
Europe & Africa	https://wwc.europe.dla.mil
Pacific	https://remote.pacific.dla.mil/
Distribution	https://rmt.distribution.dla.mil Click "Continue to the Website"

Type the URL, and click **Enter**

Note: Some users may not be required to complete steps 5 and 6 due to site-specific Citrix configuration

5. Select the **I Agree With the Statements Above** button



Hardware Textiles Medical

DEFENSE LOGISTICS AGENCY
Clothing The Warfighters Logistics Combat Support Agency

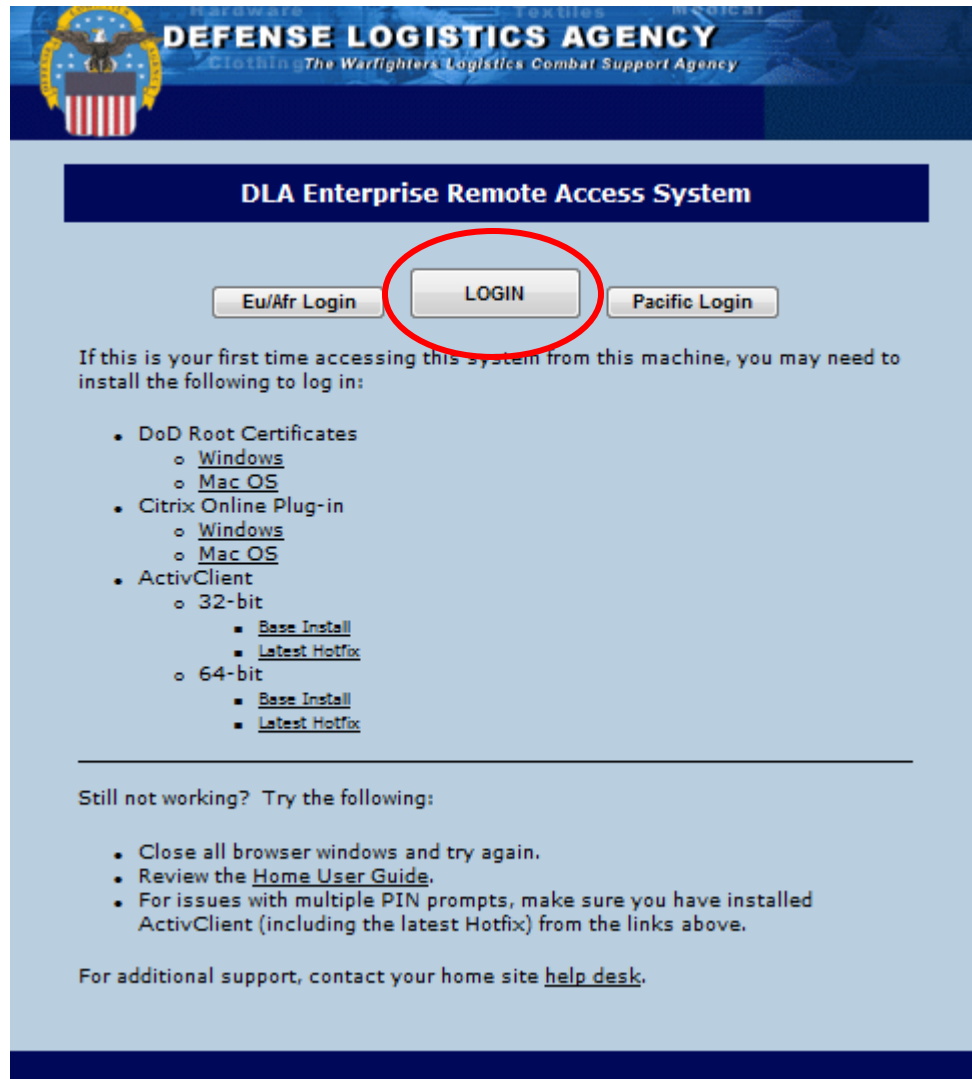
You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

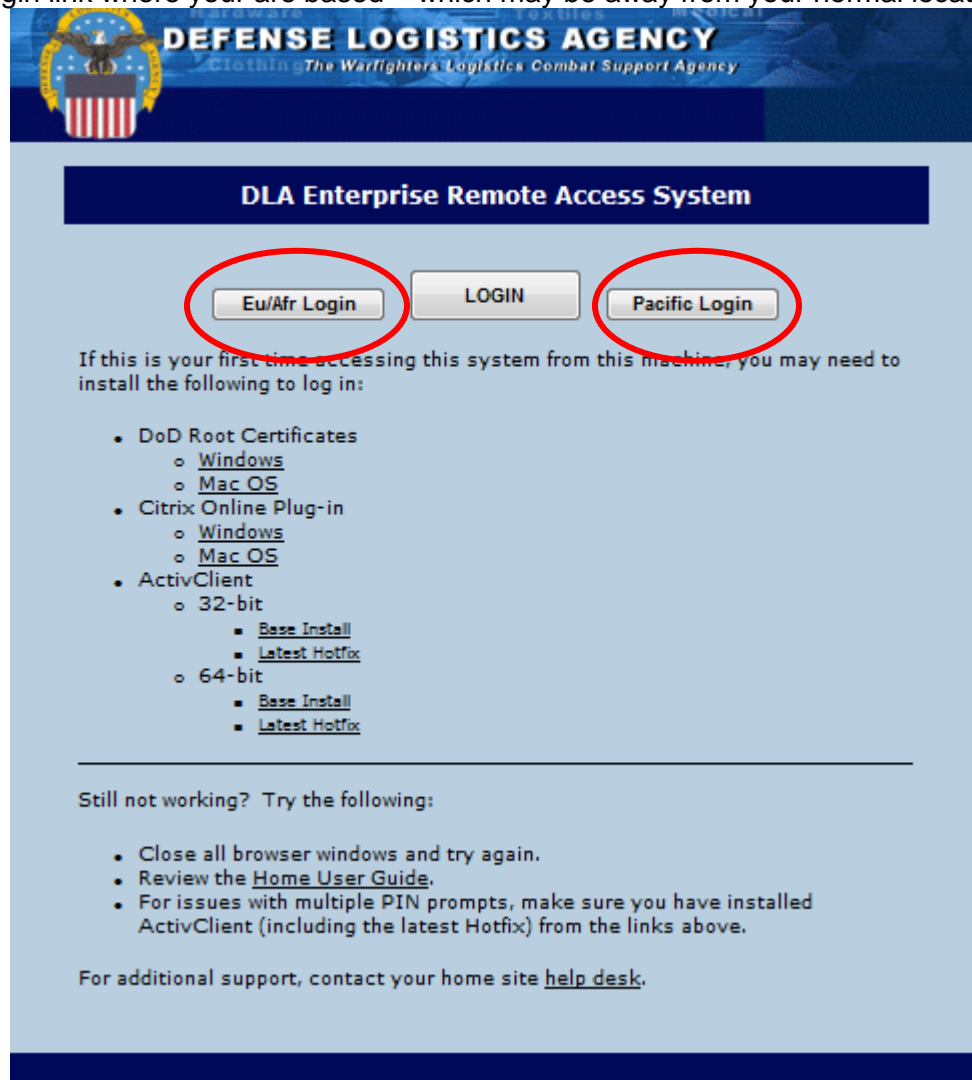
- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE, or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communication and work product are private and confidential. See User Agreement for details.

6. Select DLA Enterprise Remote Access System location

1. For CONUS Users , Select **Login** link (Note: select the login link where your are based – which may be away from your normal location)

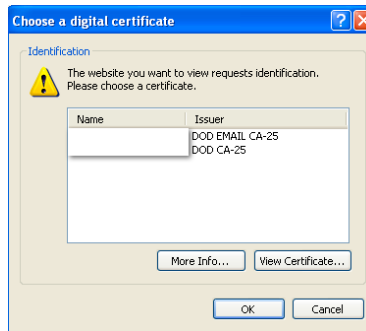


2. For OCONUS Users, Select **Eu/Afr Login** or **Pacific Login** link (Note: select the login link where you are based – which may be away from your normal location)

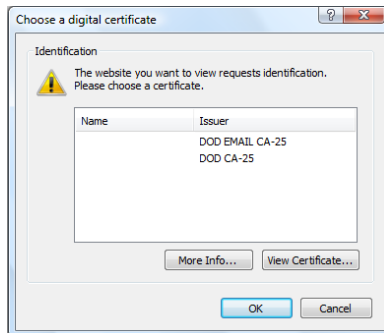


7. When prompted select your **DOD EMAIL** certificate and click **OK**

Windows XP:



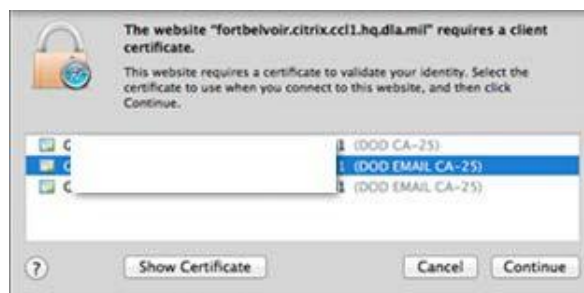
Windows Vista:



Windows 7:

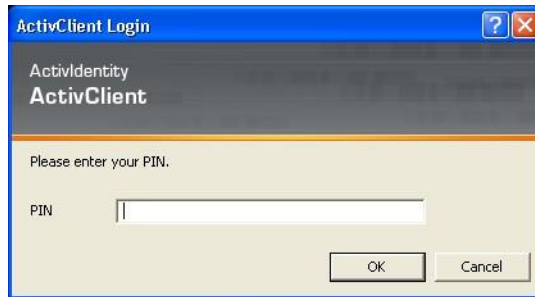


Mac OS:

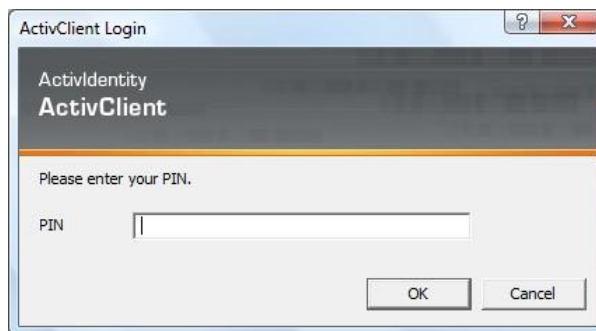


8. When prompted type your CAC

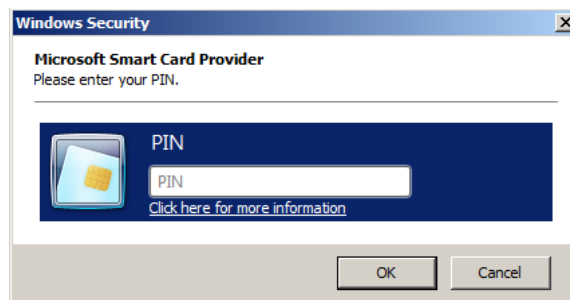
PIN: Windows XP:



Windows Vista:



Windows 7:



Mac OS:

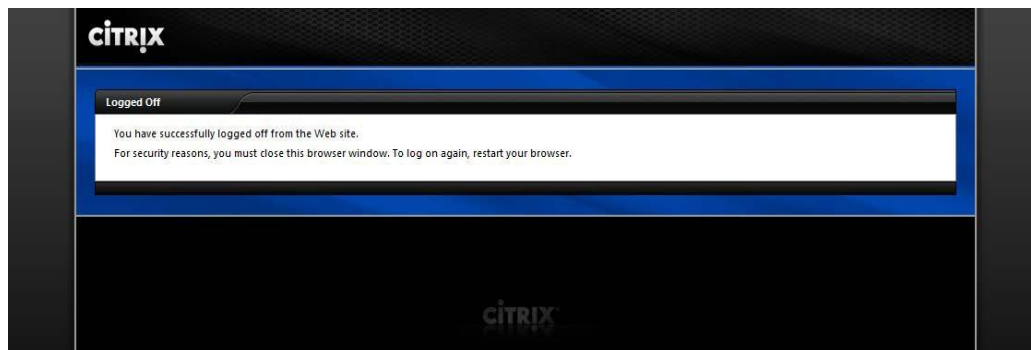
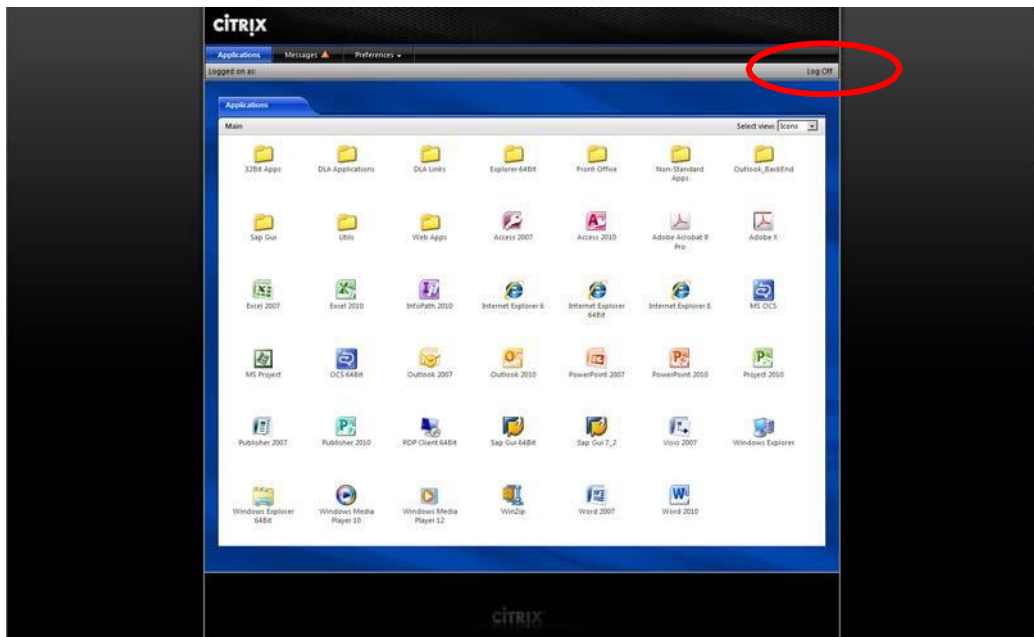


9. The next screen that appears will be the CITRIX Application window.
- (Note: The icons you see upon logging in may differ from those shown below)



10. To launch an application, single (left) click on the icon for the program you wish to launch.
- When prompted, select your Certificate and enter your PIN.

11. To Logoff, click on the **Log Off** in the upper right corner. The Web portal will log you off automatically after 20 minutes of the page being inactive. This does NOT log you out of your Citrix Session.



Appendix A – How to Establish Outlook Profile Settings

How to add a Personal Folder (i.e., PST file) to your Outlook profile



1. Open Outlook through Citrix.
2. On the **File** menu, select **Open**, and then select **Outlook Data File**.
3. Select your U: drive from the drop-down menu.
*Distribution and J6N users select H: drive and the “outlookpst” folder.
4. Double-click the .PST file that you want to open, and then click OK (you may have to navigate through your subfolders to find the appropriate file).
5. Your .PST file should now be listed in your Outlook window.

How to add an Outlook Auto Signature to your Outlook profile

1. Open a new message. On the **Message** tab, in the **Include** group, click **Signature**, and then click **Signatures**.



2. On the **E-mail Signature** tab, click **New**.
3. Type a name for the signature, and then click **OK**.
4. In the **Edit signature** box, type the text that you want to include in the signature.
5. To format the text, select the text, and then use the style and formatting buttons to select the options that you want.
6. To add elements besides text, click where you want the element to appear, and then do any of the following:

OPTIONS	HOW TO
To add an electronic business card	Click Business Card , and then click a contact in the Filed As list. Then click OK
To add a hyperlink	Click  Insert Hyperlink , type in the information or browse to a hyperlink, click to select it, and then click OK
To add a picture	Click  Picture , browse to a picture, click to select it, and then click OK . Common image file formats for pictures include .bmp, .gif, .jpg, and .png.

7. To finish creating the signature, click **OK**.

NOTE The signature that you just created or modified won't appear in the open message; it must be inserted into the message.

Appendix B – Printing With Citrix

Citrix users will be able to access a printer that is physically connected using appropriate drivers installed on the non-GFE machine.

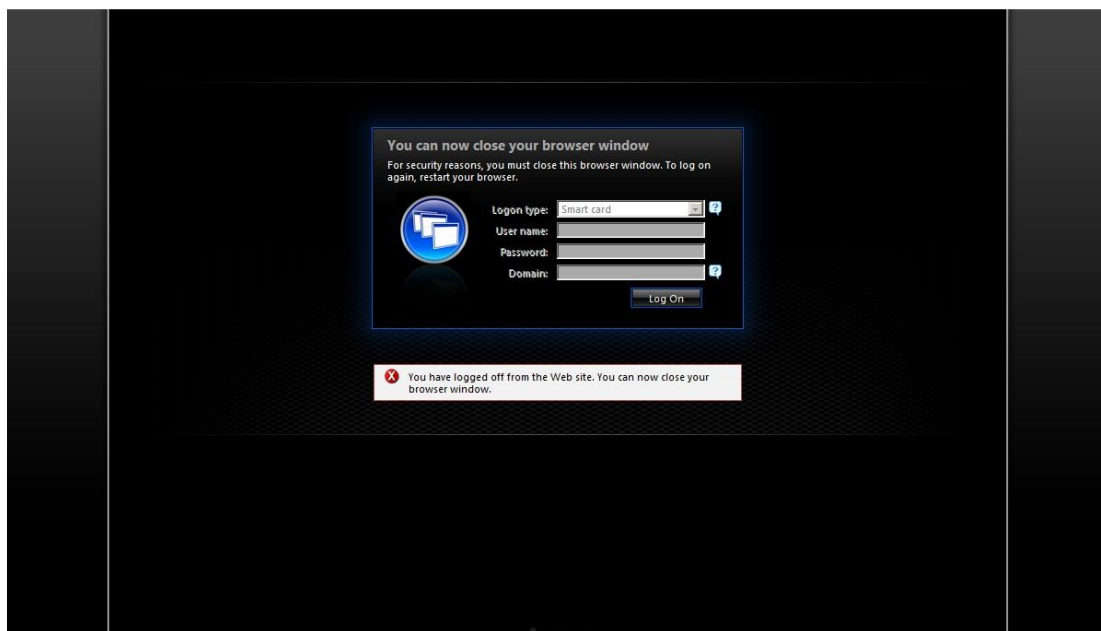
The printing device may be connected to the non-GFE machine or through the following types of connections:

Printer Connection	Enabled?
Local USB Connection	Yes
Local LPT Connection	Yes
Local Network Printer (i.e., local network printer, Wifi or LAN)	Yes
Network printer on Government network (i.e., multi-function printer at your DLA office)	No

All locally available printers will be “auto-created” in the Citrix environment and made available to the Citrix client, allowing printing to occur just as if initiated from a locally installed application. No additional action is required to print from Citrix to any locally connected printer.

Appendix C – Tips and Common Error Solutions

1. If the following screen appears, preventing the user from selecting their certificate and logging in, all browser sessions should be closed. Upon logging in with a new browser session, the issue should be resolved.

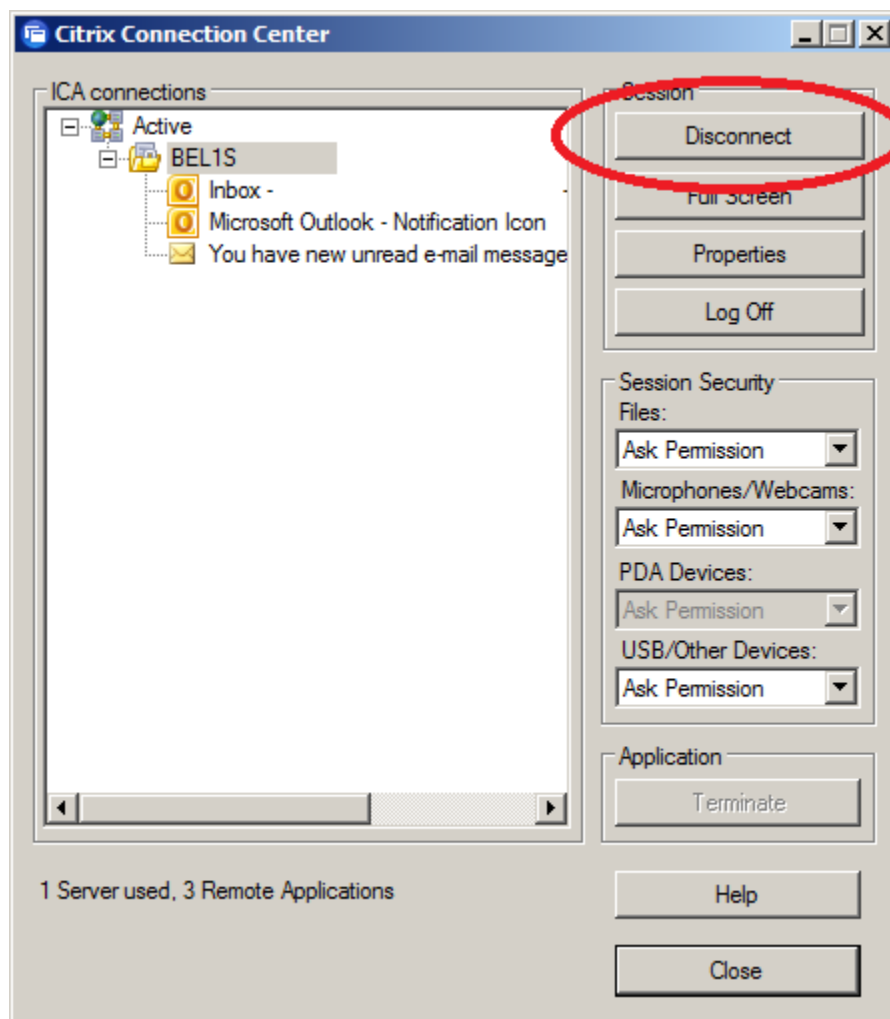


2. Occasionally in circumstances involving slow connectivity, Citrix applications may not immediately respond to attempts to launch applications. In this scenario users should refrain from repeatedly clicking the application icon as this will cause the application to 'queue up' multiple instances that will all begin launching, negatively impacting Citrix performance. If, after waiting at least 30 seconds, an application does not launch or has appeared to fail during launch, then at that point click on the application's icon again as this may result in it launching properly. Users should also note that responsiveness and performance of the Citrix application should improve after the initial connection is established and the application launches.

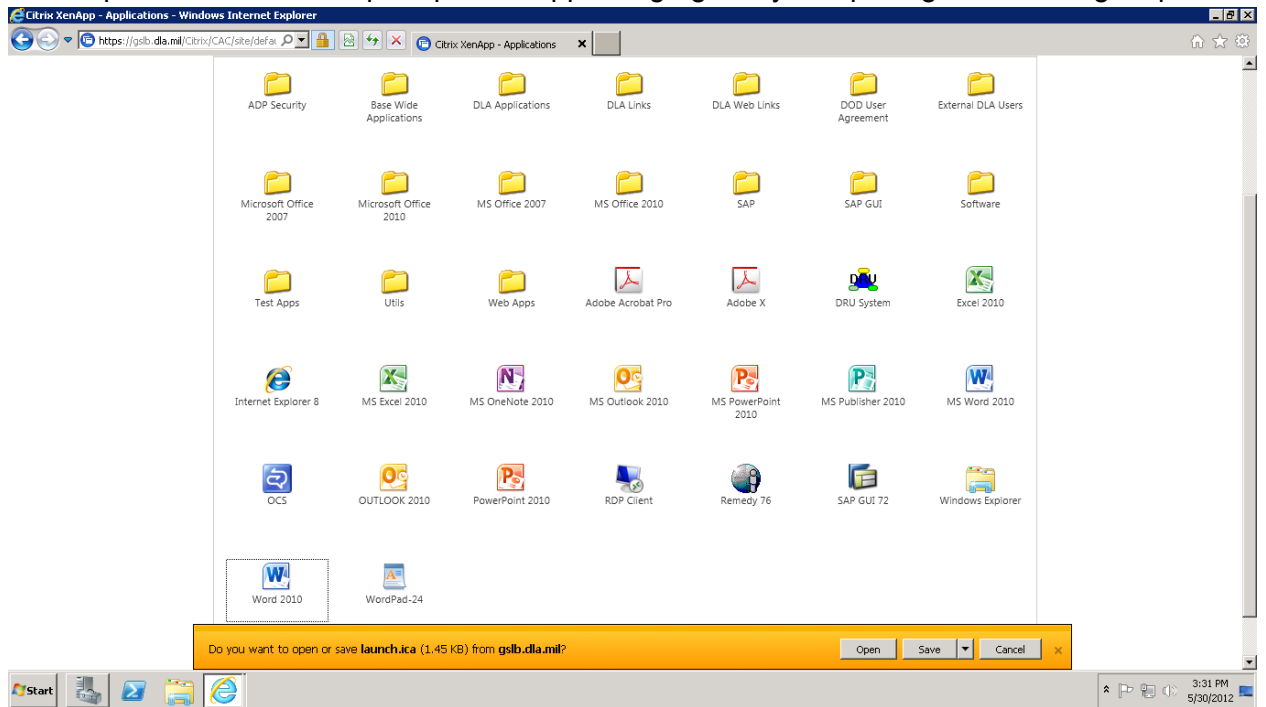
3. If you see a Windows Server account lock screen, and you are no longer using Citrix, this screen can be closed by right clicking the Citrix Connection Center icon in your System Tray and selecting **Open Connection Center**.



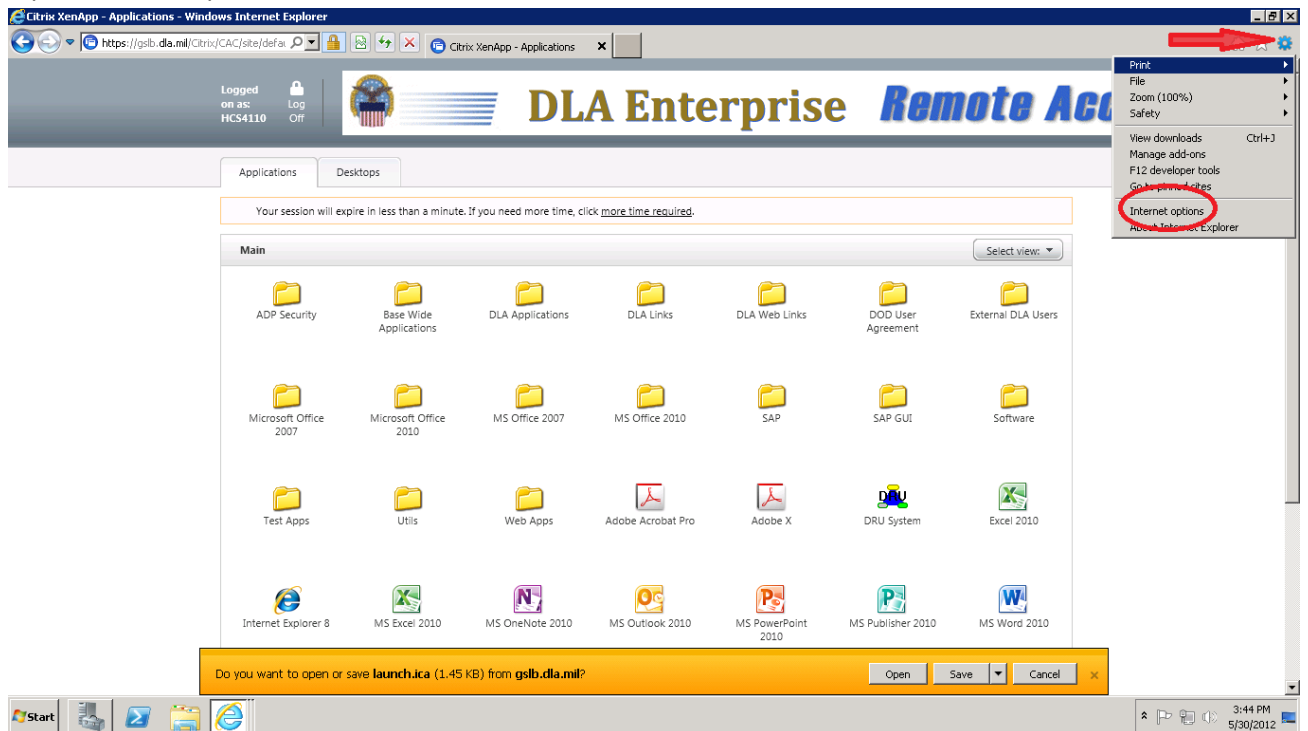
When the Citrix Connection Center Window appears, click the **Disconnect** button. This will close your Citrix session and Windows Server lock screen.



4. If you are using Internet Explorer version 9, and you receive the following prompt, you can click “Open” or remove this prompt from appearing again by completing the following steps:



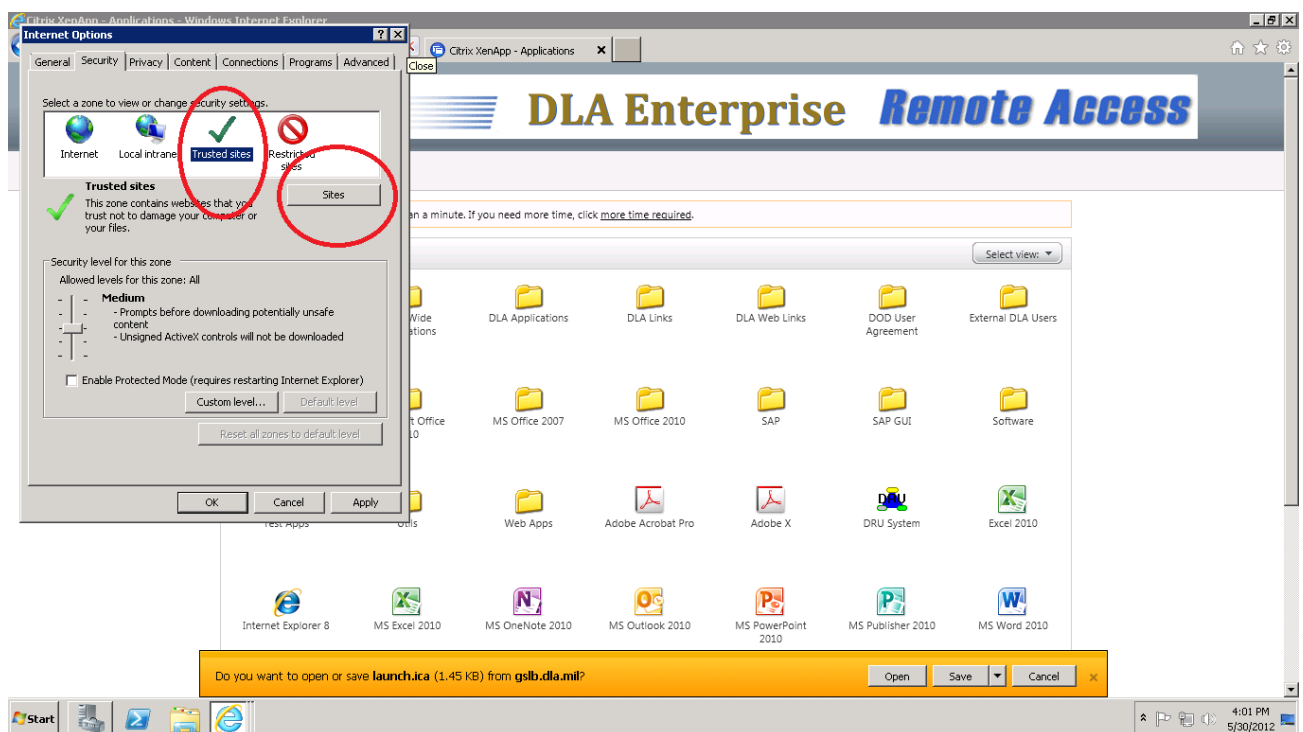
Open Internet Options:



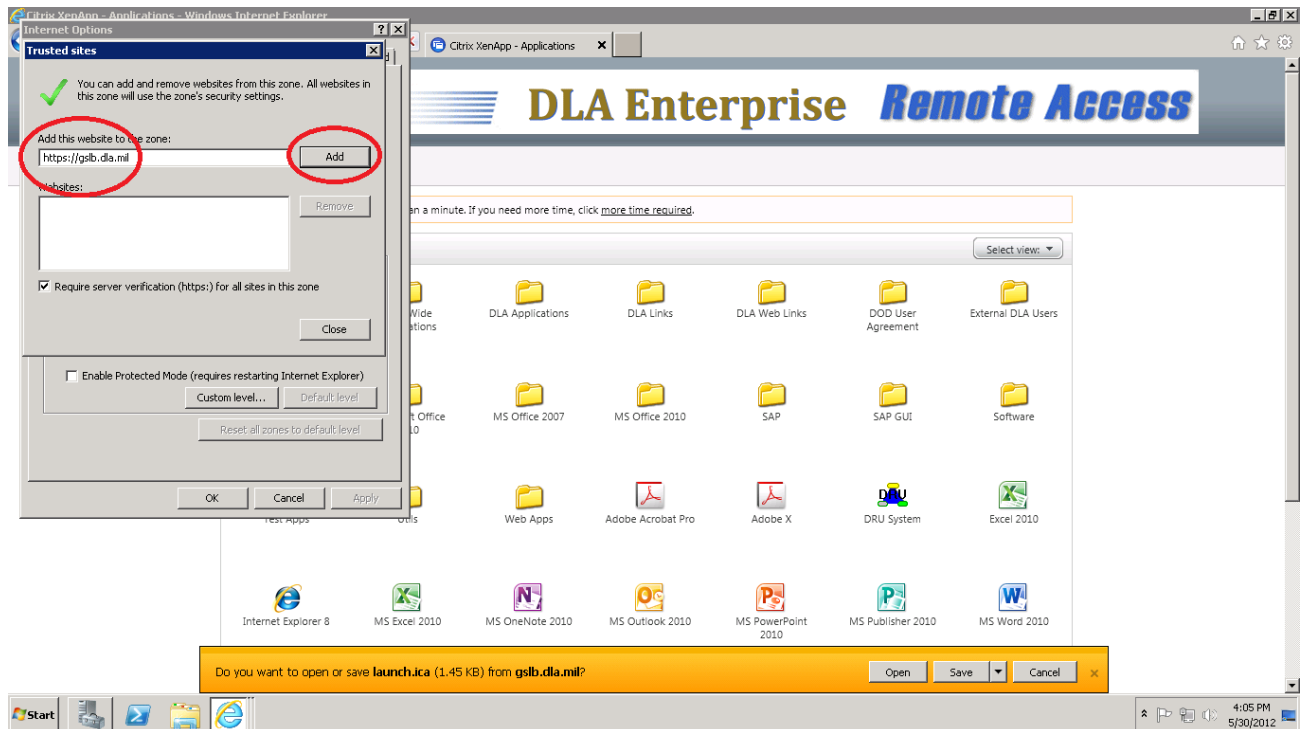
Click Security:



Click "Trusted Sites" then click "Sites":



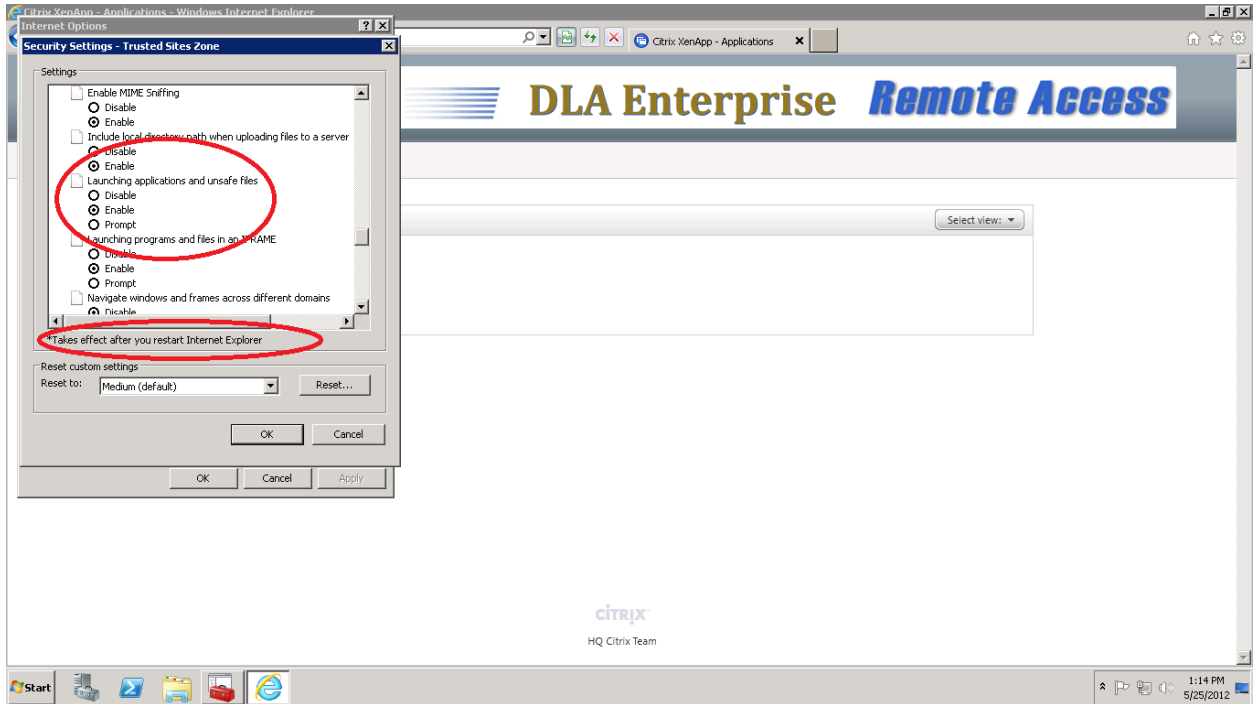
Click “Add” to add this web site then “Close”:



Select “Custom Level”:



Scroll ¾ of the way down until you see “Launching applications and unsafe files”. Select “Enable”, Select “OK” and close Internet Explorer:



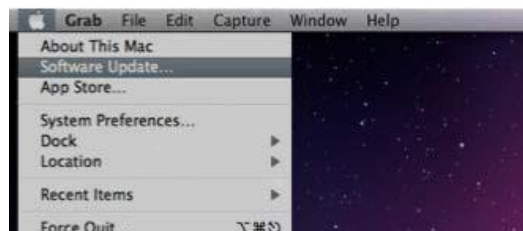
Appendix D - Instructions for Configuring and Using Citrix with Mac OS

Notes:

- **DLA Help Desk does not support any versions of Mac OS and will be unable to assist in** following or troubleshooting the steps detailed in this section of the guide. **Use at your own risk.**
- If previous attempts to configure CAC access have occurred, it may be necessary to delete existing certificates, identity preferences and keychains created by these previous attempts.
- If you are running Mac 10.6.X or 10.7.X, following these instructions you may be able to access all CAC enabled Web sites without additional 'identify preference' actions, copying certificates or creating keychains as with prior versions of Mac OS. Additionally, it may be beneficial to performance to clean prior instances of these items out of your system, allowing the system to create what it needs.

Steps 1-5 are for making your CAC function on your Mac and have been validated to work on Snow Leopard (Mac OS X 10.6.X) and Lion (Mac 10.7.X).

1. Ensure your system is updated to the latest software (currently Mac OS X 10.6.X, 10.7.X and Safari 5.1.1).



2. Plug in your CAC reader. Open your System Profiler.

From the Finder Menu: Click

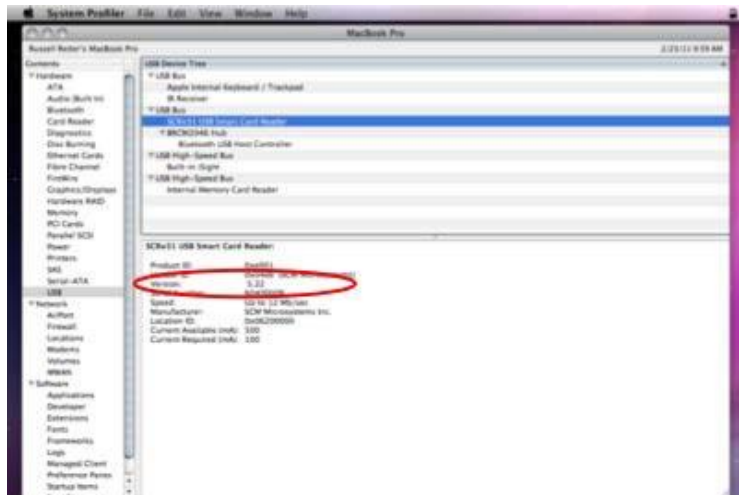
- Go
- Utilities
- Small triangle icon triangle to open it up
- Snow Leopard 10.6.X
 - Double-click System Profiler
- Lion 10.7.X
 - Double-click System Information.

NOTE: If 'Go' is not visible, click the finder icon in the taskbar or click any blank space on the desktop.

Within the "Hardware" Category select "USB." On the right side of the screen the window will display all hardware plugged into the USB ports on your Mac. "Smart Card Reader" should be visible. If the Smart Card reader is present, is installed on your system, and no further hardware changes are required (e.g., additional drivers / Firmware upgrades). You can now Quit System Profiler.

NOTE: If the version is 5.18 or 5.25 for an SCR-331 Reader, it should work fine. If it is below 5.18, please update your firmware.





3. Snow Leopard Users (Mac v10.6.X) may omit steps 3-5 and skip to Step 6.

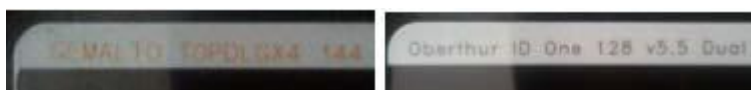
Beginning with Lion (Mac v10.7.X), Tokend modules no longer ship with the Mac OS.

10.7.X users will need to install one of the following sets of modules, dependent upon the version of CAC they are using, which can be determined by looking at the top left corner of the back of the card (as shown in the images below). If you have either of the following models of CAC (verify by looking at the top left corner of the rear of the card as shown below: or,

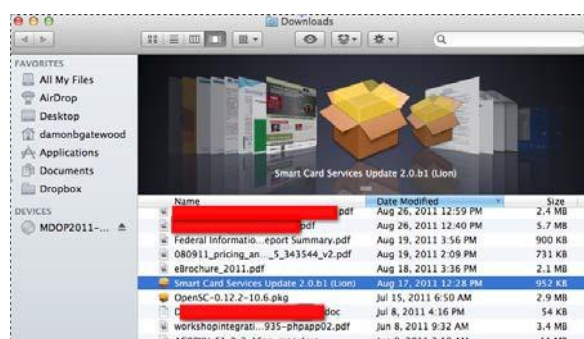
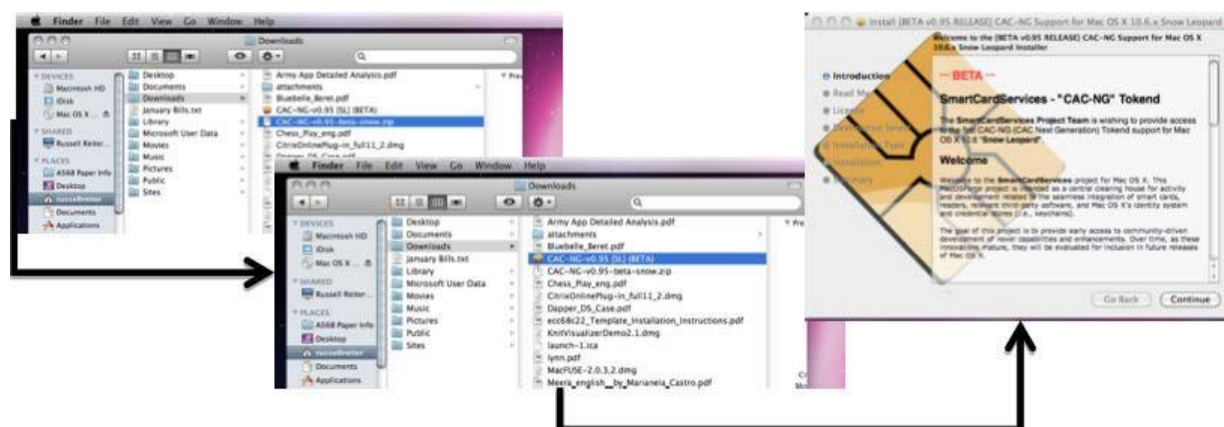
- Gemalto TOP DL GX4 144
 - Tokend module download:

<http://militarycac.com/MAC/CAC-NG-v0.95-beta-snow.zip>
- Oberthur ID One 128 v5.5 Dual
 - [http://static.macosforge.org/smartcardservices/downloads/installers/SmartCardServices_2.0.b1_\(Lion\).zip](http://static.macosforge.org/smartcardservices/downloads/installers/SmartCardServices_2.0.b1_(Lion).zip)

These links will install the necessary Tokend modules, including Belpic, CAC, CACNG, and PIV. Note that this installer will only install onto OS X Lion (Mac v10.7.X).



4. Open Finder and navigate to where you saved the file downloaded in the last step. Extract the ZIP file by double-clicking, then install the TOKENEND by double-clicking the file that is extracted.

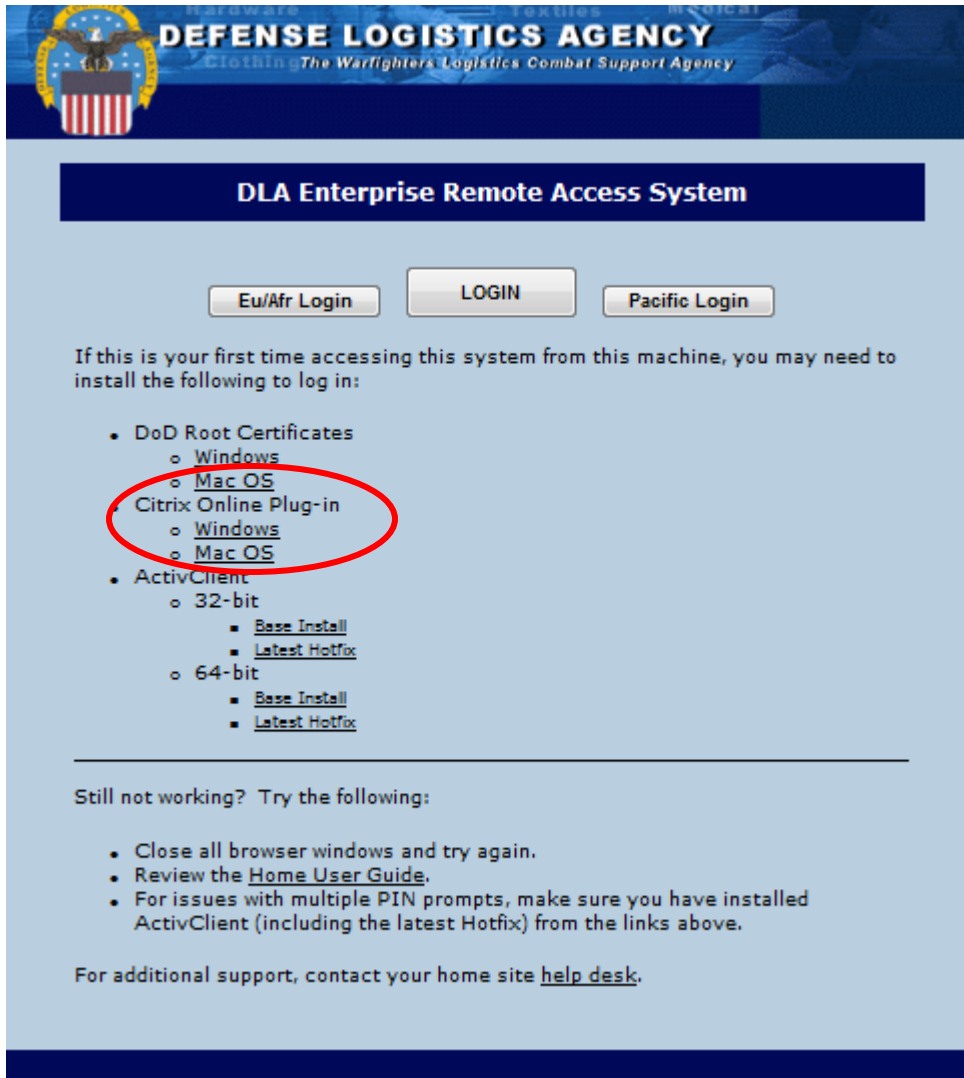


5. Restart your computer.
6. Once these steps are completed, you should be able to see your CAC in your Keychain Access. To open it, from the Finder Menu: Click Go, Utilities, click the little triangle to open it up, double click Keychain Access.

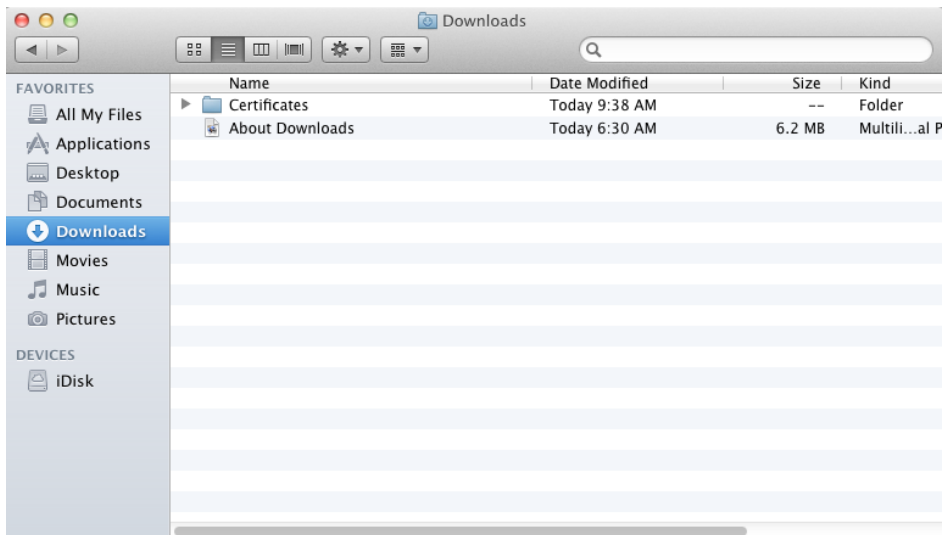
NOTE: If 'Go' is not visible, click the finder icon in the taskbar or click any blank space on the desktop.



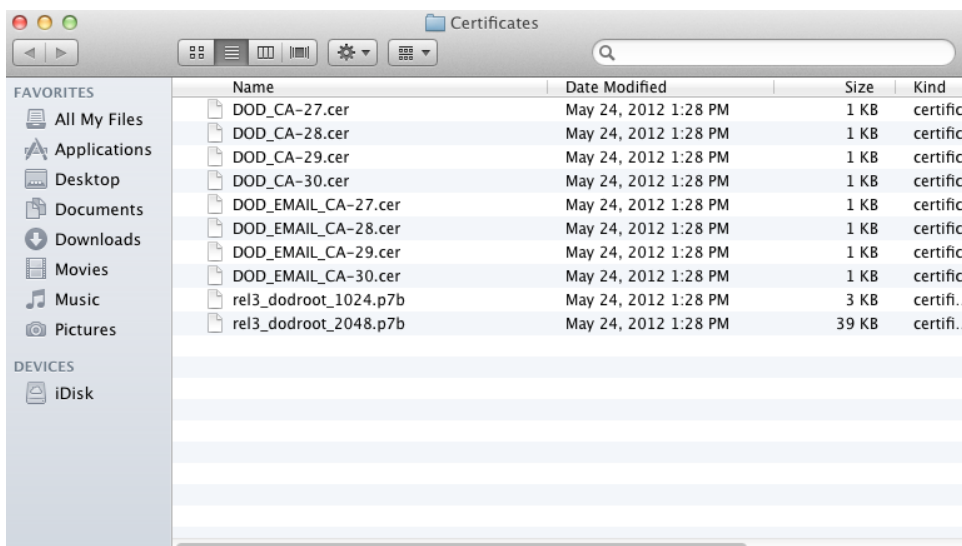
7. Select the CAC Keychain and then click the small padlock in the upper right hand corner of the Keychain access window to unlock your CAC Keychain. It will ask you for a password, this is your PIN.
8. Ensure you have DOD Certificates in your System Roots Keychain. If not, these can be downloaded from: <https://remote.dla.mil/access.html> under Mac OS and Certificates



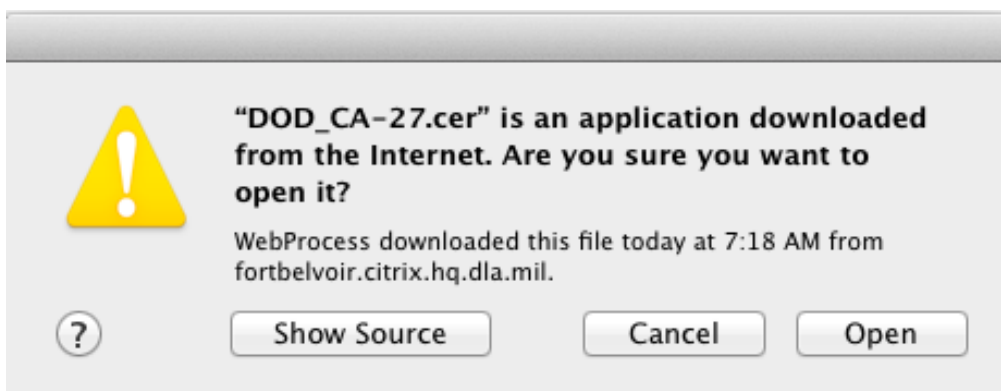
Navigate to the Downloads Folder and Select the Certificates Folder



Open Certificates Folder



Double Click on each one of the certs one at a time.



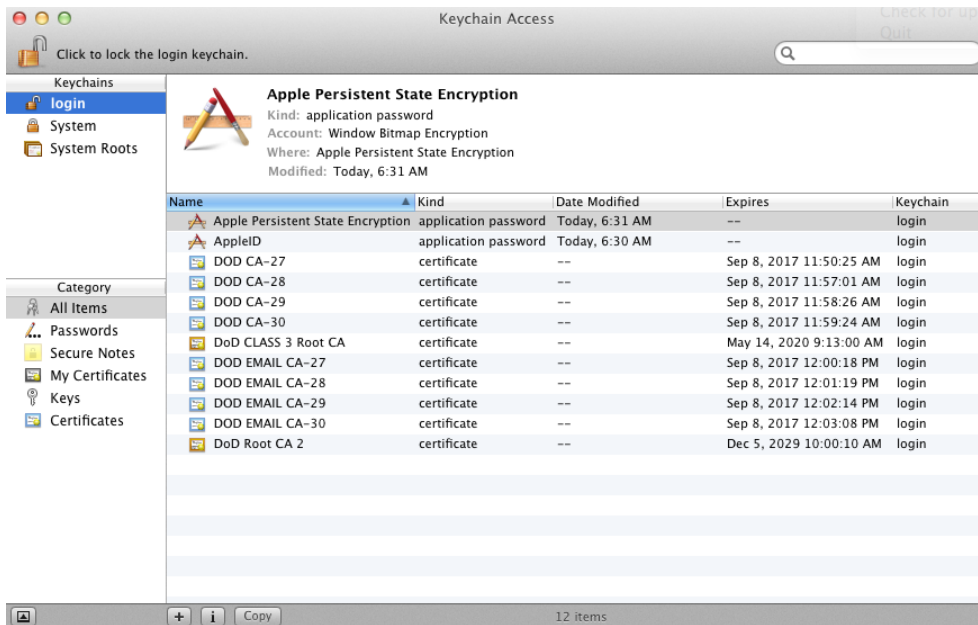
Click Open



Select Add. Keychain should be login as it appears above.



When all Certs in the Certificate folder have been executed individually your Key Chain should look the image below.



NOTE: The prior steps consist of configuring the operating system to have access to the certificates contained on the CAC; however, you cannot use the applications until you do the following steps as well:

9. Download the Citrix Online Plug-in for Mac 11.2 (or most current version) from this website:

<http://www.citrix.com/site/ss/downloads/details.asp?downloadid=2309129&productid=186>

NOTE: Make sure you get the Citrix Online plug-in For Web Access and NOT the Citrix Online plug-in For Admin Use Only

Receiver for Mac 11.2 (Online Plug-in)

Release Date: 8/26/2010

[Back to results](#)

Use the "Citrix Online plug-in for Mac – web" to access hosted applications from your Citrix Web Interface.

Use for on-demand access to Windows and Web applications using Safari or Firefox with Mac OS X 10.5 or 10.6 (Intel or PowerPC). No set up is required.

View the list of countries that may have **export or import restrictions** for products containing strong (128-bit or greater) encryption.

General Documentation

[Readme](#) | [Citrix eDocs Library](#)

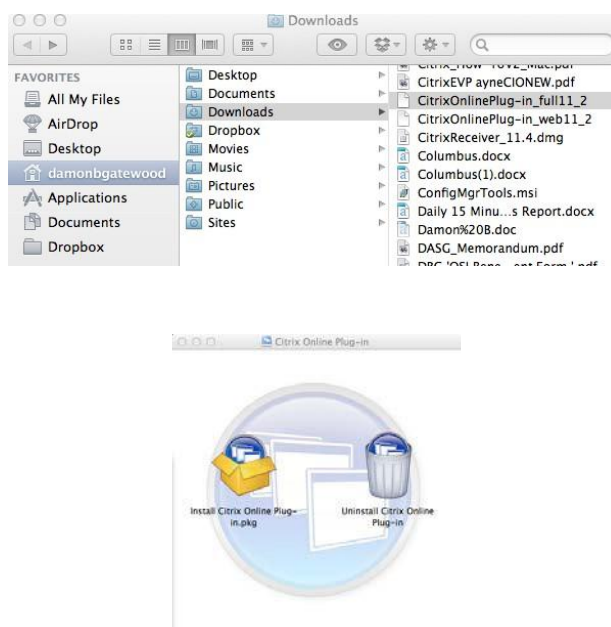
For Web Access

Product Name	Language	Release Date	Size	Format	Action
Citrix Online plug-in for Mac - Web	English	8/26/10	18.2 MB	.dmg	Download

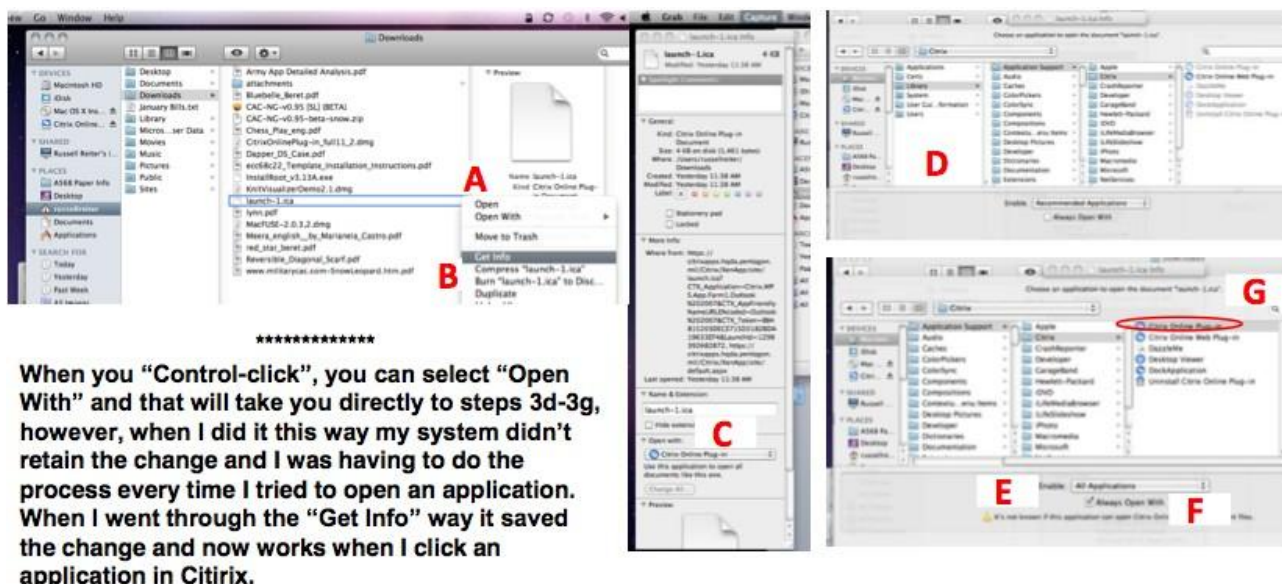
For Admin Use Only

Product Name	Language	Release Date	Size	Format	Action
Citrix Online plug-in for Mac - Admin	English	8/26/10	25.1 MB	.dmg	Download

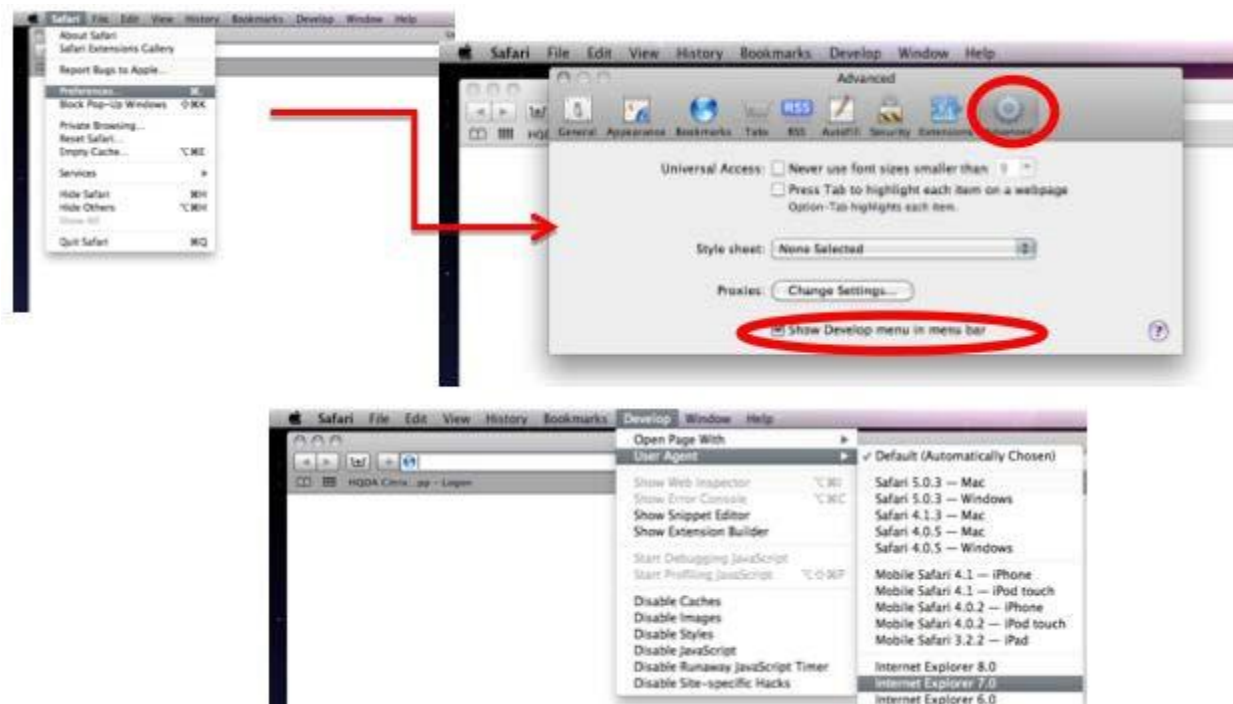
10. Open Finder and navigate to where you saved the file downloaded in the last step and install the plug-in by double-clicking the file.



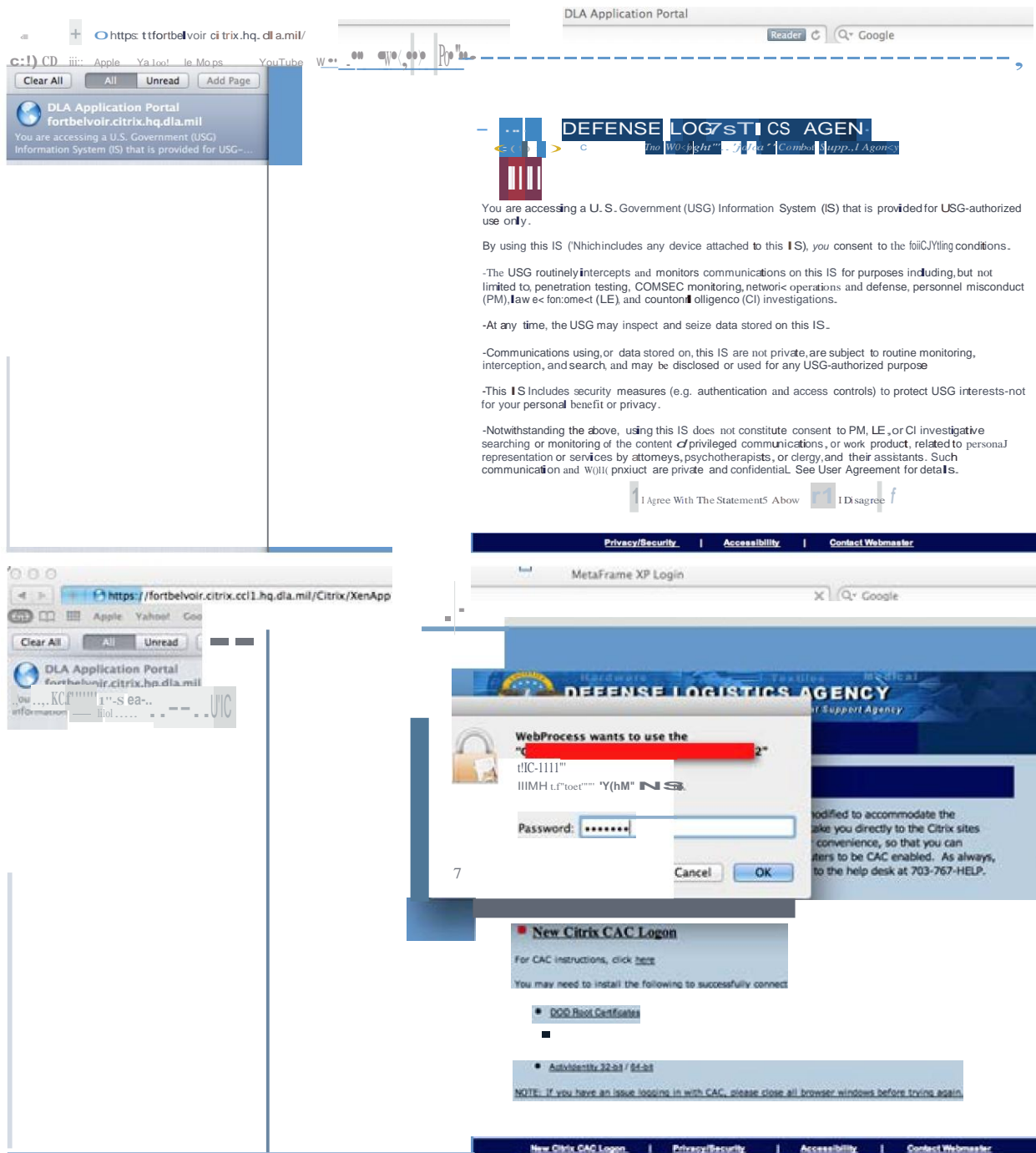
11. If, when you select an application from the Citrix Applications screen (i.e., Outlook), your system pops up a Finder window showing where it downloaded a “*.ica” file rather than opening the application, then you need to do the following (you should only need to do this one time):
- A. “Control-Click” on the *.ica file
 - B. Select “Get Info”
 - C. Go to the “Open With:” Section and select “Change All”
 - D. Navigate to MACINTOSH HARD DRIVE/LIBRARY/APPLICATION SUPPORT/CITIRX
 - E. Drop down the “Enable” box and choose ALL APPLICATIONS
 - F. Check the “ALWAYS OPEN WITH” box
 - G. Choose the “Citrix Online Plug-in” **NOT** the “Citrix Online Web Plug-in”

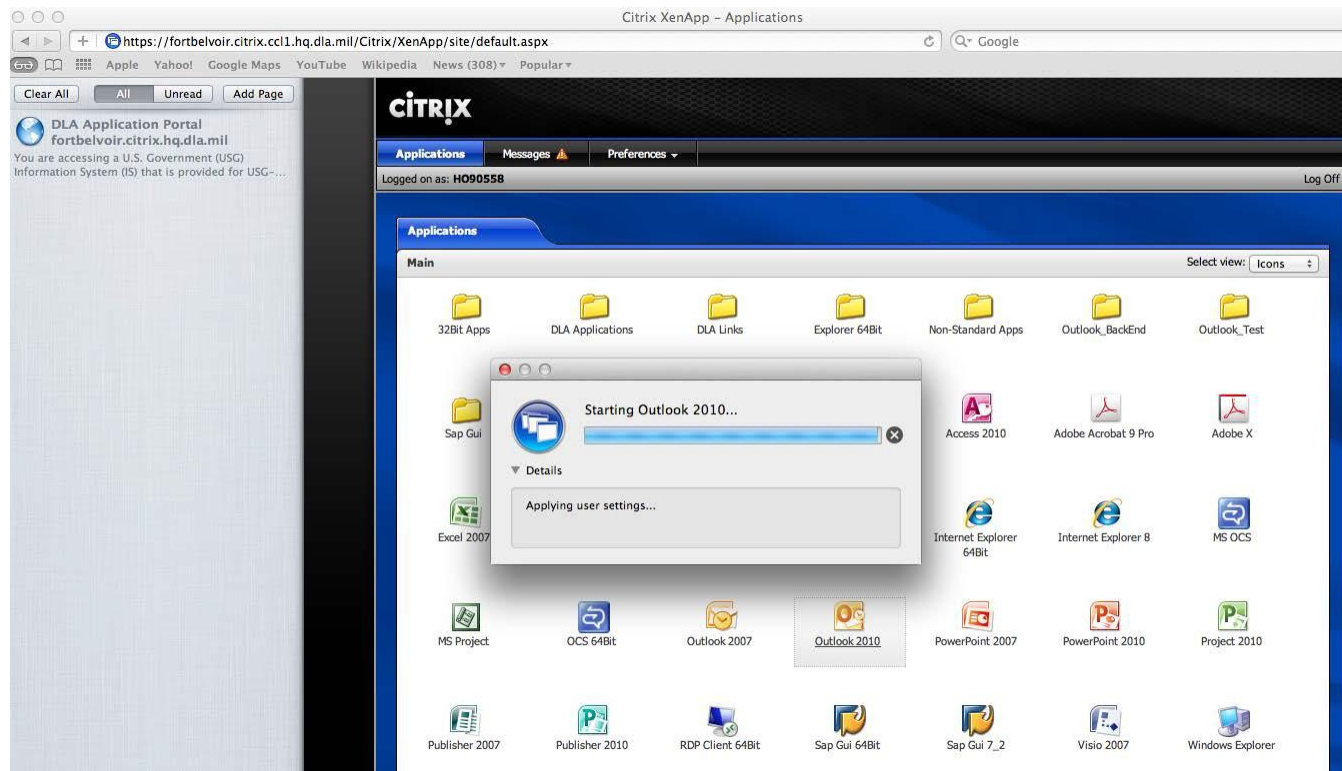


12. Open Safari, enable the Develop menu (Preferences, Advanced) and put Safari in the mode to emulate IE 7.0.



13. Navigate to DLA Citrix Logon portal and choose SMART CARD logon. Choose the first DOD EMAIL CA-## certificate when prompted.





The first time you log in, this will create two “identity preference” entries in your “Login” keychain. One for “*.mil” sites and one for <https://remote.dla.mil>”

Once these are created you will not need to choose a certificate each time you log on. If you haven’t unlocked your CAC Keychain you will be prompted for your PIN.

If you ever need to use a different certificate (i.e., you chose the wrong certificate or you get a new CAC) simply delete these two entries and when you logon again, you will be prompted to choose a certificate.

If log on fails, another attempt should be made choosing the alternate certificate.

Appendix E – Approved Smart Card Readers

Supplier	Product Name	Part Number
Cherry Electrical Products	Cherry Smart Terminal ST-1044U	ST-1044UB
Cherry Electrical Products	Cherry Smart Reader SR-4044	SR-4044
Cherry Electrical Products	SR-4300 ExpressCard Smart Card Reader	SR-4300
Cherry Electrical Products	ST-1210 SmartTerminal Smart Card Reader (XX1X)	ST-1210UAX-x
Dell Inc	Dell External USB Keyboard with Smart Card Reader	SK-3205
Dell Inc.	Broadcom USH2 Smartcard Solution	BCM5882
Dell, Inc	Broadcom USH Smart Card Solution	BCM5880
Dell, Inc.	Dell Latitude D430, D630,D830 w/ o2 Micro Smart Card	OZ77CR6
Dell, Inc.	Dell External USB Keyboard with Smart Card Reader	RT7D60
HID Corporation	iCLASS RK40	6130BKN000000-G3.0
HID Corporation	iCLASS OEM150	3121BNN0000-G3.0
HID Corporation	iCLASS RPK40	6136AKN000000-G3.0
HID Corporation	iCLASS RKL550	6170BKT000000-G3.0
HID Corporation	iCLASS RK40	6130CKN000000-G3.0
HID Corporation	iCLASS RPK40	6136CKN000000-G3.0
HID Corporation	iCLASS RMK40	6230CKN000000-G3.0
HID Corporation	iCLASS RMPK40	6236CKN000000-G3.0
HID Corporation	Omnikey 5321 USB Smart Card Reader	Omnikey 5321
HID Corporation	Omnikey 5321 CR USB Smart Card Reader	Omnikey 5321 CR
HID Corporation	Omnikey 5321 CL SAM USB Smart Card Reader	Omnikey 5321 CL SAM
HID Corporation	iCLASS RMP40	6225CKN00000-G3.0
HID Corporation	iCLASS RM40	6220CKN00000-G3.0
HID Global Corporation	iCLASS RP40	6125CKN00000-G3.0
HID Global Corporation	iCLASS R10	6100CKN00000-G3.0
HID Global Corporation	iCLASS R15	6140CKN00000-G3.0
HID Global Corporation	iCLASS R30	6110CKN00000-G3.0
HID Global Corporation	iCLASS RP15	6145CKN00000-G3.0
HID Global Corporation	iCLASS R40	6120CKN00000-G3.0
HID Global Corporation (formerly Omnikey Americas)	Omnikey 4321 ExpressCard SmartCard Reader	Omnikey 4321
Lenel Systems International	LNL-3121	LNL-3121
Lenel Systems International	Lenel OpenCard PIV Reader XF1100-PIV	LNL-XF1100D-PIV
Lenel Systems International	Lenel OpenCard PIV Reader XF2100-PIV	LNL-XF2100D-PIV

Lenel Systems International	Lenel OpenCard PIV Reader XF2110-PIV	LNL-XF2110D-PIV
SCM Microsystems Inc	SCR3500 USB Smart Card Reader	905141
SCM Microsystems, Inc.	SCR331 USB Smart Card reader	SCR331
SCM Microsystems, Inc.	SCR243 PCMCIA S/C Reader	SCR243
SCM Microsystems, Inc.	SCR3310 USB Smart Card Reader	SCR3310
SCM Microsystems, Inc.	SCR3311 USB Smart Card Reader	SCR3311
SCM Microsystems, Inc.	SCR131 Serial Port S/C Reader	SCR131
SCM Microsystems, Inc.	SCR531 Serial/USB S/C R/W	SCR531
SCM Microsystems, Inc.	SCR333 Drive Bay USB SC Reader	SCR333
SCM Microsystems, Inc.	SCR3340 ExpressCard 54 SC Reader	SCR3340
SCM Microsystems, Inc.	SDI010 Contact/Contactless Smart Card Reader	SDI010
SCM Microsystems, Inc.	PAT1312 Physical Access Reader	904565
SCM Microsystems, Inc.	PAT1322 Physical Access Reader	904566
SCM Microsystems, Inc.	SCR338 Smart Card Keyboard	903720
SCM Microsystems, Inc.	SCR3310 v2	SCR3310 v2
SCM Microsystems, Inc.	PAT1241	904322
SCM Microsystems, Inc.	SCR339	905174
SCM Microsystems, Inc.	SCR3310	905185
SCM Microsystems, Inc.	SCR3311V2	905194
SCM Microsystems, Inc.	SCR333V2	905195
SecuGen Corporation	SecuGen iD-USB SC/PIV	EA4-0516B
XceedID Corporation	Multi-Tech Wallmount Reader	XF1500P
XceedID Corporation	Multi-Tech Wallmount RS485 Reader	XF1500CS4
XceedID Corporation	Single-Frequency Mid-Range Keypad Reader	XF2210
XceedID Corporation	Single-Frequency Mid-Range Reader	XF2200
XceedID Corporation	OEM Module	OEM100
XceedID Corporation	Single-Frequency Mullion Reader	XF1200